ISSN No. 0976-5697

Volume 7, No. 1, January-February 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Analysis of Biometric Authentication System – Security, Issues and Working using Visual Cryptography

Dhara Kumari
M.Tech Scholar
SRCEM College
Palwal (India)

Dr. Rajni Sharma
Assistant Professor (Computer Science)
PT.J.L.N. Govt P.G College
Faridabad (India)

Abstract: In today's generation security of that transmitted data is most important problem because network technology is greatly advanced and lot's of information is transmitted via the internet. So this network services are now open to all so confidential data may not be safe at all through the network. It needs to be encrypted first so that if somebody manages to retrieve/capture the data from network, he shouldn't be able to decrypt the original message. Transmission of data through computer network is increasing rapidly. So the security of transmitted data is very important issue. To provide the security to transmitted data we can use Cryptography, Visual Cryptography and Biometric. This paper provides an overview of various cryptographic techniques. It indicates the problems and issues of Biometric system, and gives way out to these issues. It also gives the working of biometric authentication system.

Keywords: Network Security, Authentication, Transmission, Privacy, Visual Cryptography, Biometric

I INTRODUCTION

In today's world there is a growing concern regarding identity theft, national security, and on-line terrorism [4].The rapid development in various communication technologies, the transmission as well as immediate access to digital data or transmitted data is a common and most popular example. That's why to prevent this digital data or transmitted data to be interfered and forged by unauthorized parties is one of the most critical demand in computer' era. Whereas, authentication and encryption are crucial to network security. A traditional network security system provides a secure way to exchange information but designing a high security authentication system still remains an open problem. i.e. Complex passwords are easy to forget while a simple password is easily guessed by unauthorized persons. So this network services are now open to all so confidential data may not be safe at all through the network. It needs to be encrypted first so that if somebody manages to retrieve/capture the data from network, he shouldn't be able to decrypt the original message. The transmission of data through computer network is increasing rapidly. Thus, the security of transmitted data is very indispensable issue. To provide the security to digital data or transmitted data we can use various cryptographic techniques likes: Cryptography, Visual Cryptography and Biometric.

II CRYPTOGRAPHY

Cryptography is derived from Greek word „Krýpto which means hidden and „Grafo", which means written. It is the study and implementation of techniques to hide information (Like, written text, electronic signals, e-mail messages or data transmissions) or simply to protect a message or text from being read. Cryptography is a technique where the plain text is converted into cipher text on sender side and this process is known as encryption and the cipher text is converted into plain text on receiver side which is known as decryption process. "Fig. 1", shows the general structure of a cryptosystem.

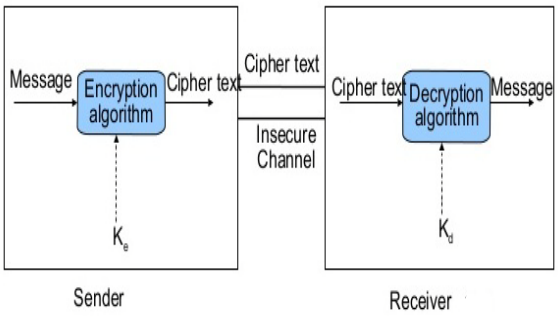

Figure1. General structure of a cryptosystem

In this technique there are two methods:

1. Symmetric key cryptography - where same key will be used for encryption as well as decryption also, but will be used in opposite manner.
2. Asymmetric key- where encryption will be done using public key which may be known to all but decryption will be done by private key that is known to the user/receiver only.

Cryptography is the study of mathematical techniques related aspects of information security such as confidentialities, data security, entity authentication, but it is not only the means of providing information security whereas the computation process should be complex enough such that nobody i.e. the intruder will be able to break the system. As computing power is becoming more and more fast, our older cryptographic systems becoming less secure because an attacker can attempt large number of random attack attempts in shorter time. Thus, Privacy protection is very important in today's world where personal information, images are generally shared to each other through the network. When we are sharing information on internet number of outsiders or intruder try to hack it before the

information is received by the receiver. So, to protect the information from hackers visual cryptography scheme is used that was introduce by [1] Moni Naor and Adi Shamir in 1994 which allows visual information like pictures, text, data to be encrypted in such a way that decryption becomes a very easy operation that does not require any type of computation or computer.

III VISUAL CRYPTOGRAPHY

Visual Cryptography is an encryption technique based on the secret sharing problem. In this case, visual information is shared, i.e., the message to be encrypted can be a black and white image, grey scale or a colored one, printed text, etc. The encryption of the secret is done in such a way, that its decryption is very simple since there is no need for any mathematical calculations: it is done automatically by the human eye. Thus, we can say that Visual cryptography is one of the techniques used to encrypt the images by dividing the original image into transparencies. The transparencies can be sent to the intended person, and at the other end the transparencies received through the person can decrypt the transparencies using the tool, thus gets the original image. "Fig. 2", shows the general structure of a visual cryptography.

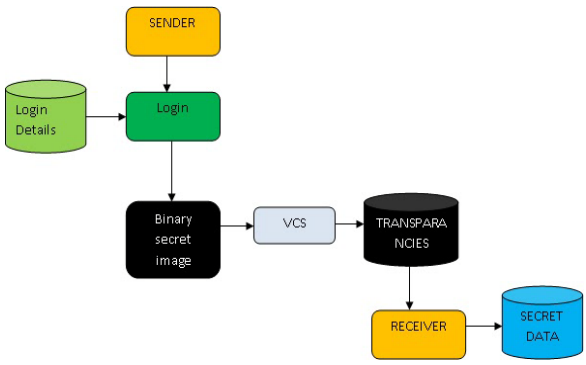

Figure2. General structure of a visual cryptography

During this procedure we can apply various types of visual cryptography scheme (VCS). The VCS describes the way in which an image is encrypted and decrypted.

For example, there is the k-out-of-n scheme that says n shares will be produced to encrypt an image, and k shares must be stacked to decrypt the image [3]. If the number of shares stacked is less than k, the original image is not revealed. The other schemes are 2-out-of-n and n-out-of-n VCS. In the 2-out-of-n scheme n shares will be produced to encrypt an image, and any two shares must be stacked to decrypt the image. In the n-out-of-n scheme, n shares will be produced to encrypt an image, and n shares must be stacked to decrypt the image. If the number of shares stacked is less than n, the original image is not revealed. Increasing the number of shares or participants will automatically increase the level of security of the encrypted message. This scheme work on Two-out-of-Two Scheme (2 subpixels layer) and Two-out-of-Two Scheme (4 subpixels layer) using the "OR" and "XOR" operation.

For example, explanation of Two-out-of-Two Scheme (2 subpixels layer):

The encoding scheme is to share a binary image into two different shares Share 1 and Share 2. Each pixel is divided into a black and white subpixel placed next to each other. For the case of white pixel, one of the two combinations of subpixels will be chosen with a probability of 0.5 to represent the pixel in each of the shares. When these shares are placed one on top of the other, the pixel are visually ORed[1] and hence a white pixel looks gray (half black and half white) to the human eye.

[1]The term "ORed" as used in this paper refers to when two values are combined, they are bitwise ORed together.

The pixels are chosen in a similar manner for the case of a black pixel. But when the subpixels are visually ORed, the two black subpixels placed next to each other appear as a single black pixel. This idea can be applied to images to develop a basic Two-out-of-Two scheme by using 2 subpixels. The 2 out of 2 visual secret sharing problems can be solved by the following collection of $n \times n$ matrices:

C0 = {all the matrices obtained by permuting the columns of $\begin{bmatrix}0 & 1\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\1 & 0\end{bmatrix}$ }

C1 = {all the matrices obtained by permuting the columns of $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$ }

Pixel		Share 1	Share 2	Result
	P = 1/2			
	P = 1/2			
	P = 1/2			
	P = 1/2			

Figure3. Partitions for black and white pixels for 2-out-of-2 scheme (2 subpixels)

visual cryptography scheme is one of the most secure techniques for privacy protection, that allow the encryption of secret image or data by transferring it into the secure share and such a scheme is able to recover the secret image or data without any computation devices. Basically, visual cryptography has two important features. The first feature is its perfect secrecy and the second is its decryption method which requires neither complex decryption algorithms nor the aid of computers. It uses only human visual system to identify the secret from the stacked image of some authorized set of shares. Therefore, visual cryptography is a very convenient way to protect secrets when computers or other decryption devices are not available.

During the analysis, visual cryptography has two important drawbacks.

- Visual cryptography scheme (VCS) is that even a layman to cryptography is able to decode the secret image without having any cryptographic knowledge and computational tools/devices.
- Visual cryptography scheme (VCS) is the loss in contrast of reconstructed image.

Now-a-days, recognizing person using alphanumeric passwords is not sufficient for the identity determination because they can be easily guessed or stolen. Therefore this situation and drawback of visual cryptography is removed by using the concept of Biometric System where Biometric is one of the authentication and generally pattern recognition system it comes from the Greek words "bios and metricos" which means "life measure" that determines person based on his physiological characteristic.

It is more reliable, convenience, reliability, universality, consistent and also user friendly. So it is used for many application such as computer login control, passport control, border crossing, secure e-banking, ATM, credit card, airport, etc.

Visual cryptography enables to derive from an image two shares that give separately no information on the original image while leading back to the image by superimposition of the shares. This technique can be applied to explore the plausibility of using visual cryptography for imparting privacy to biometric templates such as finger-print images, iris codes, and face images. In the case of faces, private face image is dithered into two host face images (known as sheets) that are stored in two separate database servers such that the private image can be revealed only when both sheets are simultaneously available; at the same time, the individual sheet images do not reveal the identity of the private image.

IV BIOMETRIC

Biometric is the science of establishing the identity of an individual based on physiological or behavioral traits [2]. "Fig. 3", shows the physiological or behavioral traits.

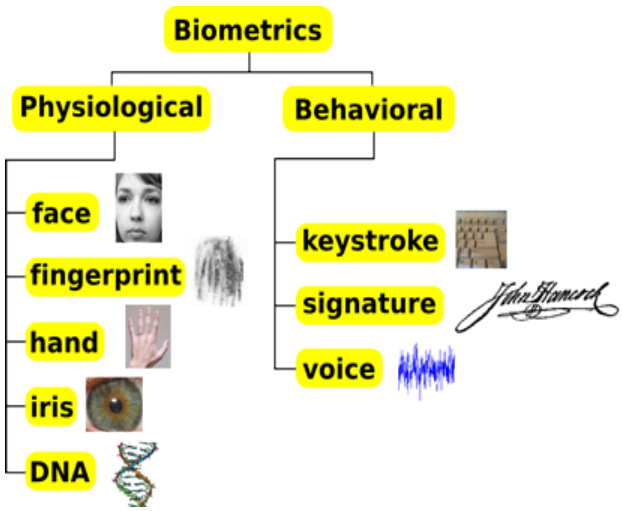

Figure4. Physiological or behavioral traits.

- Physiological Biometrics: It is based on direct measurements of a part of the human body. Fingerprint, face, iris, and hand scan recognition belong to this group [5].
- Behavioral Biometrics: It is based on assortments and data derived from an action performed by the user, and thus indirectly measures some characteristics of the human body. Signature, gait, gesture, and key stroking recognition belong to this group [5].

This technology brings a new dimension to individual identity verification that provides a guaranteed level of accuracy and consistency over traditional methods.

"Fig. 4", shows the general model of biometric system.

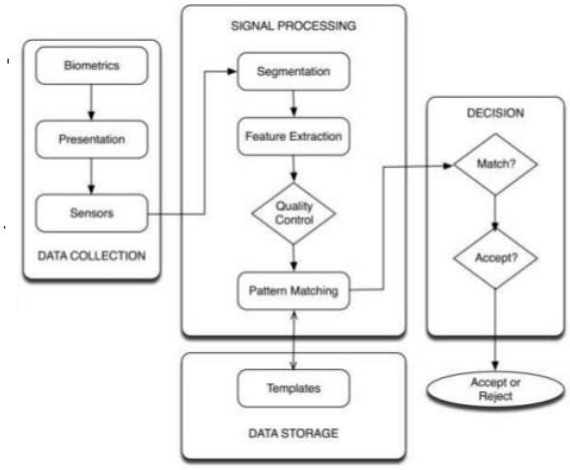

Figure5. General model of biometric system.

The working of biometric authentication system acquires raw biometric data from a subject, extracting a feature set from the data, and comparing the feature set against the templates stored in a database in order to identify the subject or to verify a claimed identity.

V ISSUES OF BIOMETRIC SYSTEM

At the same time there is a possible for intruder to access the database which stored the biometric data. So the security and privacy of biometric system is a major concern due to their issues like fake biometric, override matcher etc.

- **Fake Biometric: -** Attack on the sensor. Sensor can be overridden by presenting fake like fake finger, face mask or a copy of signature.
- **Replay Old Data: -** The Attack on the channel between the sensor and the feature extractor. Biometrics which was submitted can be resubmitted or replayed by bypassing the sensor like an old copy of fingerprint or face image.
- **Override Feature Extractor: -** Feature extractor can be override by attacking it and forcing it to produce feature values selected by the hacker.
- **Override Matcher: -** Attack on the matcher. Matcher can be overridden by attacking it and forcing it to produce high or low matching score irrespective of the input.

Solution Approaches for this situation:

There are following approach that can be used to obtain a solution for the above mentioned problem/situation.

- Steganography Techniques for Biometric Template Security.
- Watermarking Techniques for Biometric Template Security.
- Visual Cryptography Technique for Biometric Template Security.

VI WORKING OF BIOMETRIC AUTHENTICATION SYSTEM

Biometric ergonomics and Visual cryptography security are highly complementary, hence the motivation for their integrated application. Known methods for generating cryptographic keys from biometric measurements can be characterized as having two stages.

- In the first stage, features of raw input are used to compute a bit string.
- The second stage develops a cryptographic key from the bit string.

If two bit strings are sufficiently similar, then the same cryptographic key will be generated from them. Several techniques fitting this two-stage structure have been proposed for generating cryptographic keys from biometrics. Biometric recognition, as a means of personal authentication, is an emerging signal processing area focused on increasing security and convenience of use in applications where users need to be securely identified. Biometric characteristics are inherently associated with a particular individual, making them insusceptible to being forgotten or lost.

Therefore, Visual Cryptography and biometrics have been identified as the two most important aspects of digital security. Visual cryptography enables to derive from an image two shares that give separately no information on the original image while leading back to the image by superimposition of the shares. In this work, we apply this technique to explore the plausibility of using visual cryptography for imparting privacy to biometric templates such as finger-print images, iris codes, and face images. In the case of faces, private face image is dithered into two host face images (known as sheets) that are stored in two separate database servers such that the private image can be revealed only when both sheets are simultaneously available; at the same time, the individual sheet images do not reveal the identity of the private image.

Below "Fig. 5", shows an example of the working of biometric system (Fingerprints) using the concept of visual cryptography. A similar technique is used for face images.

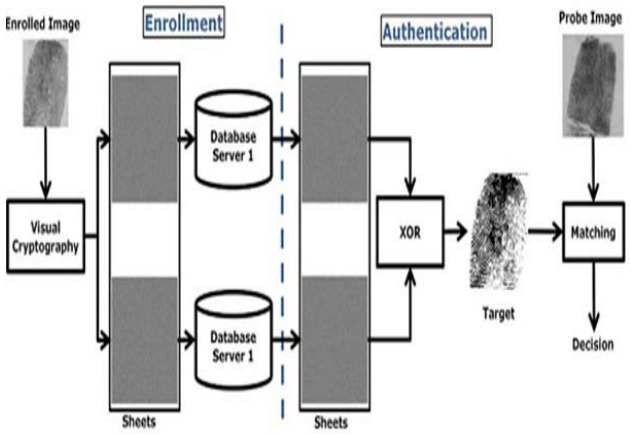

Figure6. Working of biometric system (Fingerprints) using the concept of visual cryptography. A similar technique is used for face images.

A biometric authentication system operates by acquiring raw biometric data from a subject (e.g., face image), extracting a feature set from the data (e.g., Eigen-coefficients), and comparing the feature set against the templates stored in a database in order to identify the subject or to verify a claimed identity. The template in the database is generated during enrollment and is often stored along with the original raw data.

VII CONCLUSION

Visual Cryptography and Biometrics can play an essential role, reinforcing security at all stages where people authentication is needed.

In the early stage, the presence of users and devices, where the same user might want to access to interactive media contents from different environments (such as home, car, work, jogging, etc.) and also from different devices or media (such as CD, DVD, home computer, laptop, PDA, 2G/3G/4G mobile phones, game consoles, etc.) strengthens the need for reliable and universal authentication of users. Traditional user authentication systems have been based in something that you have (like a key, an identification card, etc.) or something that you know (like a password, or a PIN). Whereas, with biometrics, a new user authentication paradigm is added: something that you are (e.g., fingerprints or face) or something that you do or produce (e.g., handwritten signature or voice).

Future work can be achieved by using 2-out-of-2 VCS with 4-subpixel layout using the Embedded Extended Gray-level Visual Cryptography Scheme (EEGVCS) that is based on the XOR and XNOR operation. It also works on the central database for biometric information (like face, fingerprints, and iris). In this work, the basic VCS is used to secure iris ciphers and fingerprint images and the Embedded extended VCS for grayscale images is used to secure face images. The future work will cover the Multi level visual secret sharing technique, how the pixel expansion rate will be reduced and in what way high quality target image will be obtained which indeed increases the storage requirements for sheets and the target image. It will support 2D, 3D, .bmp, .png and .gif etc formatted images. Thus, the system's security will also be improved by hiding multiple secrets in same number of share images and reduces the size of sheets and share image.

VIII REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12

[2] A. Jain, P. Flynn, and A. Ross, Handbook of Biometrics. New York: Springer, 2007.

[3] Adhikari Avishek and Bimol Roy (2007). "Applications of Partially Balanced Incomplete Block Designs in Developing (2,n) Visual Cryptographic Schemes". IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences Vol.E90-A No.5 pp.949-951

[4] J. Abbazio, S. Perez, D. Silva, R. Tesoriero, F. Penna and R. Zack, Proc. Student-Faculty Research Day, CSIS, New York, USA, pp. C1.1-C1.8 (2009).

[5] S.Sumathi and R.RaniHema Malini research Scholar,Sathyabama University,Chennai-96 An Overview of Leading Biometrics for Human Identity15. Oxford English Dictionary. Oxford Edition, 2004.

[6] Stinson, D. 1995. Cryptography Theory and Practice. CRC Press.

[7] Alfred, J, Paul, C and Scott, A. 1965. Handbook of Applied Cryptography, Library of Congress Cataloging-in-Publication Data.

[8] Katoh, T. and Imai, H. 1996. Some Visual Secret Sharing Schemes and Their Share Size. Joint Conference of 1996 International Computer Symposium, Kaohsiung, Taiwan, R.O.C., pages 19- 21.

[9] Alfredo De Santis, On Visual Cryptography Schemes, Proc. of the IEEE ITW 1998, pp. 154-155, 1998.